

ORIGINAL

United States District Court  
NORTHERN DISTRICT OF TEXAS

**FILED**  
SEP - 2 2010  
CLERK, U.S. DISTRICT COURT  
CRIMINAL COMPLAINT

UNITED STATES OF AMERICA

v.

JASON NEFF

CASE NUMBER B:10 m 303-BK

I, ALLYN LYND, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. From in or about January 2004, and continuing through in or about May 2008, in the Northern District of Texas and else where, defendant Jason Neff

in violation of 18 U.S.C. § 371, did,

knowingly combine, conspire, confederate, and agree with one or more persons to commit offenses against the United States, to wit: (1) to knowingly use, traffic in, possess and control hardware and software, knowing it had been configured to modify telecommunication identifying information associated with and contained in a telecommunications instrument so that such instrument could be used to obtain telecommunications service without authorization in violation of 18 U.S.C. §1029(a)(9); and (2) to intentionally access a protected computer, as that term is defined at 18 U.S.C. §1030(e)(2)(B), without authorization, and as a result of such conduct, recklessly cause damage in violation of 18 U.S.C. §1030(a)(5)(A)(ii).

in violation of 18 U.S.C. § 1512(k), did,

knowingly combine, conspire, confederate, and agree with one or more persons to commit offenses against the United States, to wit: to knowingly use intimidation, threaten, or corruptly persuade witnesses in a proceeding in the NDTX, or attempt to do so, or engage in misleading conduct toward the potential witnesses, with intent to hinder, delay, or prevent the communication to a law enforcement officer or judge of the United States of information relating to the commission or possible commission of a Federal offense, in violation of 18 U.S.C. §1512(b)(3), or otherwise obstruct, influence, or impede any official proceeding or attempt to do so, in violation of 18 U.S.C. §1512(c)(2).

I further state that I am a Special Agent of the Federal Bureau of Investigation, and that this complaint is based on the facts set out in the attached affidavit.

  
ALLYN LYND  
Special Agent  
Federal Bureau of Investigation

Based upon this complaint, this Court finds that there is probable cause to believe that an offense

Case 3:11-cr-00152-L Document 1 Filed 09/02/10 Page 2 of 27 PageID.2  
has been committed and that the defendant has committed it. Sworn to before me, and  
subscribed in my presence

September 2, 2010

Date

at

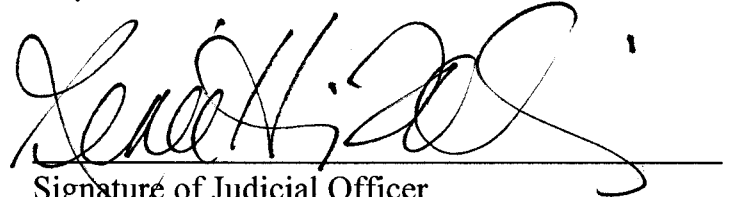
DALLAS, TEXAS

City and State

RENÉE HARRIS TOLIVER

United States Magistrate Judge

Name and Title of Judicial Officer

  
Signature of Judicial Officer

### **AFFIDAVIT IN SUPPORT OF COMPLAINT**

I, Allyn Lynd, having been duly sworn, depose and state as follows:

1. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed for approximately 13 years. I am currently assigned to the Dallas Office of the FBI, and my duties include the investigation of computer intrusions, theft of trade secrets violations, copyright and trademark infringement violations, and high-tech fraud. I have received specialized training in the field of computer intrusions and intellectual property crimes.

2. I make this affidavit in support of an application by the United States of America for the issuance of a complaint and arrest warrant for

**JASON NEFF**, also known as "CrazyJ," "Cl0pz," and "Cl0pz420" date of birth xx/xx/1981, Social Security Number xxx-xx-0970, (currently incarcerated in Camden County, Missouri, on charges of Sodomy and Child Molestation)

3. As set forth herein, there is probable cause to believe that **JASON NEFF**, also known as "CrazyJ," "Cl0pz," and "Cl0pz420," member of "globalHell," "Milw0rm," "partylinegaga," and various other computer hacking and phreaking groups, along with others individuals known and unknown to the government have conspired to engage in and/or did engage in a charging a conspiracy to violate 18 U.S.C. § 371 (18 U.S.C. §§ 1029(a)(9); 1030(a)(5)(A)(ii); and 1030(a)(2)(A)) and § 1512(k) (18 U.S.C. §§ 1512(b)(3) and 1512(c)(1) and (2)).

APPLICABLE CRIMINAL STATUTES

4. The pertinent provisions of the applicable criminal statutes are set forth below:

**§ 371. Conspiracy to commit offense or to defraud United States**

A person commits an offense when he or she and at least one other person:

conspire either to commit any offense against the United States . . .  
and one or more of such persons do any act to effect the object of the  
conspiracy, each shall be [punished in accordance with law].

**§ 1029. Fraud and related activity in connection with access devices**

A person commits an offense when he or she:

(9) knowingly uses, produces, traffics in, has control or custody of,  
or possesses hardware or software, knowing it has been configured  
to insert or modify telecommunication identifying information  
associated with or contained in a telecommunications instrument so  
that such instrument may be used to obtain telecommunications  
service without authorization.

**§ 1030. Fraud and related activity in connection with computers.**

A person commits an offense when he or she:

(a)(5)(A)(ii) intentionally accesses a protected computer without  
authorization, and as a result of such conduct, causes damage . . .

**§ 875. Interstate communications:**

A person commits an offense when he or she

(d) with intent to extort from any person, firm, association, or  
corporation, any money or other thing of value, transmits in interstate  
or foreign commerce any communication containing any threat to  
injure the property or reputation of the addressee or of another or the  
reputation of a deceased person or any threat to accuse the addressee  
or any other person of a crime, shall be fined under this title or  
imprisoned not more than two years, or both.

**§ 1512 Tampering with a witness, victim, or an informant**

A person commits an offense when he or she and at least one other person:

**1512(k)** conspire[] to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

A person commits an offense when he or she

**1512(b)** [] knowingly use[s] intimidation, threaten[s], or corruptly persuade[s] another person, or attempt[s] to do so, or engages in misleading conduct toward another person, with intent to –

(3) hinder, delay, or prevent the communication to a law enforcement officer ... of the United States ... of information relating to the commission or possible commission of a Federal offense...

**1512 (c)** [] corruptly—

(1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or

(2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so,

5. I make this affidavit in part on:

a. personal knowledge based on my participation in an investigation into the activities of **JASON NEFF**,

b. upon oral and written reports provided to me by coconspirators, victims, and witnesses who I believe to be truthful and reliable as set forth herein, and to have a sufficient basis of knowledge/access to the information that was provided to me,

c. upon the information provided to me by other law enforcement personnel,

- d. upon the information provided to me by Verizon, AT&T, and other telecommunications companies, and
- e. upon my knowledge and experience.

Since this affidavit is being submitted for the limited purpose of securing a Complaint and Arrest Warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that **JASON NEFF** has committed and is planning to commit violations of 18 U.S.C. § 371 (18 U.S.C. §§ 1029(a)(9); 1030(a)(5)(A)(ii); 1030(a)(2)(A)) and 18 U.S.C. § 1512(k) (18 U.S.C. §§ 1512(b)(3), (c)(1), and (c)(3) .

Facts not set forth in the affidavit are not being relied upon for probable cause.

#### FACTS IN SUPPORT OF AFFIDAVIT

6. Affiant first became aware of **JASON NEFF** in September 1998, when FBI Dallas received a complaint from the Dallas County Community College District (DCCCD) alleging that their phone systems, which were operated by a computer system known as "Latitude," had been compromised by unknown individuals. These unknown individuals used the compromised phone system to initiate and conduct teleconferences. DCCCD sustained significant losses due to the bills generated from the unauthorized use of the compromised phone system. Affiant assisted in the investigation, and determined that members of a group known as "globalHell," also known as (aka) "milw0rm" had caused the compromise and that the same group was responsible for multiple other similar intrusions. The DCCCD computer equipment recorded some of the unauthorized

telephone conference calls and from these recordings, Affiant learned that the conferences were used to coordinate further computer intrusions and to conduct credit card fraud. By March 1999, total losses for all victims attributed to the group were between \$1,000,000 and \$2,000,000. Affiant analyzed the calls and uncovered hundreds of conference participants, but only a few dozen responsible for the intrusion and organizing the conferences. One of the responsible individuals was identified as **JASON NEFF**, aka "Cl0pz" and "Cl0pz420." In May 1999, the FBI executed multiple search warrants at the residences of the responsible individuals, including **NEFF**'s residence in Omaha, Nebraska. The FBI obtained confessions from 10 of the individuals interviewed during the searches. The only individual who did not provide a confession was **NEFF**. At that time **NEFF** was 18 years old, living with his parents, and according to the agents on the scene, **NEFF** was uncooperative and verbally abusive to both his parents and FBI personnel. During the search of his residence, the FBI seized documents containing numerous credit card numbers and computer evidence.

7. "GlobalHell" members and associates retaliated for the searches by conducting a denial of service attack<sup>1</sup> (DDoS) on the FBI's web page and other related Department of Justice web pages. The DDoS caused the FBI web page to be unavailable for an extended period.

---

<sup>1</sup> A DDoS attack is where a 'hacker' causes multitude of systems to attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

8. The investigation into “globalHell” resulted in successful prosecutions in the NDTX. The United States Attorney’s Office chose not to pursue prosecution of **NEFF** due to his age.

9. Prosecution of **NEFF** was declined on two other occasions. In 1999 FBI Omaha investigated a matter involving computer fraud. The Omaha matter was closed in 2001 as to **NEFF** due to his minor role in the criminal conduct. In 2002 a cooperating witness (CW) provided information that **NEFF** was initiating teleconferences using stolen credit cards. The matter was closed when the CW was unwilling to testify.

10. In 2003 FBI Denver investigated **NEFF** for placing false 911 calls to police offices in Idaho. FBI Denver’s investigation was incorporated into FBI Dallas’s investigation, which involved a larger group engaged in “swatting<sup>2</sup>.”

11. In early October 2006, Detective Thompson of the Fort Worth Police Department (FWPD) advised Affiant that on October 1, 2006, the FWPD had responded to what it believed was an emergency 911 telephone call requiring an immediate police response in Fort Worth, Texas. The caller identification for the 911 phone call requesting assistance was the phone number assigned by the telephone company to the apartment resident. Upon arriving at the residence, law enforcement officers learned that the residence was an address that they had previously responded to for a false 911 call for assistance on another occasion. Detective Thompson told Affiant that FWPD had interviewed SP, the

---

<sup>2</sup> A “swatting 911 call” was a false 911 call made to police in which a false report of a violent crime was made in order to elicit a police Special Weapons and Tactics squad (SWAT) response to the physical address of a targeted individual, his or her family members, or place of employment.



apartment resident. SP told FWPB as follows:

- a. SP denied making the false 911 call and stated that the false 911 call had been made by a group of party liners<sup>3</sup> SP knew for the purpose of harassing SP.
- b. These types of harassment calls were known by SP and the members of the group as "swatting" calls. SP identified the group of individuals as Guadalupe Santana Martinez, Stuart Rosoff, and Jason Trowbridge.
- c. The "swatters" possessed the skill and means to spoof, or mask, their caller identification numbers (caller i.d.) in order to make it appear as if the false 911 call for emergency services had originated from phone numbers for the individuals who they were harassing so that the emergency calls appeared genuine.
- d. The "swatter" who had caused the false 911 call to the FWPB on that occasion was Guadalupe Santana Martinez.
- e. SP's parents had been harassed by the "swatting" group prior to the actual "swat."

12. In November 2006, SP advised Affiant of the following:

- a. SP had belonged to this group and had participated in telephone conference chats with them on a regular basis.
- b. One of the group members was **JASON NEFF**, a.k.a "CrazyJ." NEFF ran a

---

<sup>3</sup> A telephone party line was a type of telephone conference which members accessed by calling a local or toll free telephone number. The ostensible purpose of the party line was to provide a social network for individuals, many of whom were located in different states, to visit and socialize. The party line permitted a limited number of members to visit in an open conference "room" or to visit in smaller numbers in separate private "rooms" if they elected to do so, similar to Internet Relay Chat rooms, but on the telephone.

website called either patylinegaga or partylinegugu. This site documented the activities of the members of the swatting group, and posted photos of the members.

c. Matthew Weigman was one of the party line members most skilled in compromising telephone systems.

d. Jason Trowbridge was a participant in the false 911 call to the FWPD on that occasion (along with Guadalupe Santana Martinez).

e. The members of the group called the practice of directing local law enforcement to respond to an address for a false 911 call for harassment "swatting" as their goal was to have a SWAT team respond in full regalia, with guns drawn, which would alarm the residents.

f. Generally the group members would harass and threaten the individual they were going to "swat" in the days and weeks leading up to the "swat" in order to increase the terror in the victim as they knew the "swat" was going to occur but did not know when.

g. One of the telephone systems or telephone conference groups which the "swatters" used to communicate was known as either the "Jackie Donut" or the "Seattle Donut." The party lines known as "the Loach" and Sentura Chat were used also.

h. Guadalupe Santana Martinez and the others altered their caller i.d. information so that it would appear as if they were calling from a telephone company employee's phone to have service turned on or off at a physical location.

13. Affiant learned from SP's parents and other victims of the swatting incidents that the "swatters" often targeted family members, employers, landlords, etc. of the ultimate victim as a way of both increasing that victim's fear and trying to get that victim fired / thrown out of the apartment, etc.

14. In January 2007, FBI Agents arrested Martinez on a complaint out of the Northern District of Texas. Martinez confessed and admitted to participating in the conspiracy. In or about April 2007 Guadalupe Santana Martinez waived indictment and pled guilty to swatting SP, thereby verifying SP's account of the swatting. Martinez also admitted that Stuart Rosoff, Jason Trowbridge, Chad Ward, and others had participated in the false 911 call. Martinez confirmed that the named individuals and others used the party lines to coordinate their activities.

15. Through consent and search warrants, Affiant obtained recordings of some of the harassing calls placed to SP and to SP's parents prior to the false 911 call. Trowbridge, Weigman, and Angela Roberson participated in the harassing calls and threatened SP. At the time of these calls, Roberson lived with Trowbridge. Roberson previously had been in a relationship with **NEFF**.

16. In early October 2006, the Johnson County, Texas, Sheriff's Office (JCSO) advised Affiant that the JCSO had received a false 911 emergency call in June of 2006 from someone claiming to be JP, SP's father. The caller told the 911 operator that he had been using controlled substances, he had an AK-47 assault rifle, he had shot his wife, and he wanted \$50,000 or he would kill his child and any police who tried to stop him. The

phone number identified the call as coming from the home of JP in Johnson County, Texas. Law enforcement dispatched a SWAT team to the location, and learned that the call had been a hoax. The JCSP interviewed JP. JP denied making the 911 call and stated that for about two weeks he had been receiving harassing phone calls from members of a phone chat line group who were mad at his child SP. The party liners made threats and stating that they would be executing a hoax 911 call to his residence. JP said that the party line members wanted to harass SP's family in order to make SP to cease participating in the phone chats.

17. Martinez admitted to Affiant that Martinez was the one who had made the June 2006 false 911 call to JP, using a spoofcard<sup>4</sup> account to hide his caller identification information. Caller ID (CLID) is an identifying number in a telephone, which is an access device. Altering it through the use of hardware or software (such as a spoofcard) with the intent to obtain services to which the user would not otherwise be entitled, such as 911 services, constitutes a violation of 18 U.S.C. § 1029(a)(9). The threats made over the party line constitute violations of 18 U.S.C. §875(d).

18. Based on the above, Affiant conducted records checks in 2006 on Martinez, Rosoff, Trowbridge, **NEFF**, and Weigman. Numerous complaints had been lodged with the FBI against all of them for telephonic harassment, extortion, unauthorized termination

---

<sup>4</sup> A "spoofcard" is a type of commercial account accessible either online or by telephone which provides an access device, i.e. a number or computer code, which enables the caller to elect a number of services including the concealment of the caller's true Caller I.D. by substituting another Caller I.D., changing the caller's voice to another gender, and/or recording the call on the company's servers.

of telephone services, and “swatting”. During this investigation, Affiant learned that Chad Aaron Ward was a member of the group. Martinez, Rosoff, **NEFF**, and Ward had extensive criminal histories including numerous charges for making false 911 emergency services calls, false bomb threats, and telephone harassment. Martinez had charges pending against him in Kent, Washington. Affiant confirmed that the **NEFF** used the nicknames/screen names “CrazyJ” was and “Cl0pz.” Criminal History checks of **NEFF** showed that he had convictions and adverse findings against him from Washington State, including a 6/11/2002 misdemeanor for obstruction of a law enforcement officer, a 6/27/2002 misdemeanor for possession of marijuana, and 3 malicious mischief citations between 2000 and 2002 for littering, domestic violence, and harassment. In Iowa, **NEFF** has also been arrested on 9/29/1999 for obstructing the police.

19. On or about October 10, 2006, AT&T investigators advised Affiant as follows:
  - a. AT&T was familiar with the group using the “Donut” telephone chat line, (identified by SP as the “swatting group”), and could provide background information on the group.
  - b. Members of the “Donut” group were engaged in conduct to gain unauthorized access to the telephone network for the purpose of harassment and theft of services.
  - c. Members of the “Donut” group used a variety of methods for gaining access to the phone system including plain old telephones, cell phones, and Voice over Internet Protocol (VoIP).

d. Members of the "Donut" group employed a number of means to hide their identities when using the phone system to include software on their computers for altering and modifying their caller i.d. so that they could obtain services they would not otherwise be entitled to, and a commercial service for altering caller i.d. called "Spoofcard."

e. Members of the "Donut" group modified one of two pieces of identifying information contained within the telephonic devices to further their schemes, that is the CLID (caller i.d. number). Members purchased hardware for this purpose and used access devices designed to do this. (SP confirmed this during the interview with Affiant).

f. The computer equipment used by AT&T and other telephone companies in switching and controlling telephone calls are protected computers used in interstate commerce and communication as defined in 18 U. S. C. §1029(e)(2).

g. Members of the "Donut" group also modified their own telephone subscriber information so that they could "swat" someone more successfully.

h. AT&T believed that Guadalupe Santana Martinez and the others involved in the group were using multiple means of modification to include both custom written software and a service known as a "spoofcard" to accomplish the alterations.

i. Members of the group committed identity theft in order to further their scheme, and that AT&T employees were being victimized by the swatting group by the misappropriation of the AT&T employees' identities and passwords in order to

make the swatting group's illegal accesses to telephone company computers equipment appear more legitimate.

j. Weigman had registered telephone service for himself at his physical address in Boston, Massachusetts by using the identity of an AT&T employee.

20. Defendants in 3:07:CF-196-B<sup>5</sup> (Rosoff, Trowbridge, Ward, and Roberson); 3:07-111-K (Martinez); and 3:08-CR-171-M (Weigman, Nalley, and Benton) all pled guilty and confirmed that they used spoofcards and various other means to spoof their numbers or conceal their identities. Affiant conducted a records check and it appeared as if service at the address which Weigman used for telephone service was in the name of an AT&T representative, not Weigman. Affiant reviewed records and learned that Trowbridge and others used a commercial database to obtain personal identifying information of many of the victims. Trowbridge operated a debt collection agency that had access to the database for the sole purpose of use in collecting debts. Trowbridge exceeded that access by using the database to gather information on his victim in violation of 18 U.S.C. § 1030 and shared that information with his coconspirators.

21. Affiant knows that the computer equipment used by commercial database services in providing information are protected computers used in interstate commerce and communication as defined in 18 U. S. C. §1029(e)(2).

---

<sup>5</sup> In June 2007, a NDTX grand jury returned an indictment in *United States v. Rosoff, et al.* charging the defendants with conspiracy to commit access device and computer fraud, in violation of 18 U. S.C. § 371 (18 U.S.C. §§ 1029 (a)(9) and 1030 (a)(5)(A)(iii)).

22. On or about November 21, 2006, cooperating witness (CW1) advised Affiant as follows:

- a. Weigman used the nickname of "little hacker."
- b. CW1 had telephone conversations with Weigman since early 2006. In October 2006, Weigman told CW1 that Weigman used his unauthorized access to a telephone company Network Operations Center (NOC) and the computers located there, to terminate phone services to individuals. (Affiant identified a phone number originating at Weigman's address as one which was used to gain unauthorized access to Frontier Telecommunications NOC in Rochester, New York from approximately October 2006 through November 2006).
- c. Weigman had claimed to have this access by a variety of means, including social engineering, a technique used by hackers to obtain confidential information and passwords through the impersonation of authorized individuals.
- d. Weigman, Martinez, Rosoff, Trowbridge, **NEFF** and others belonged to the "swatting" group and that they cooperated together via computer and telephone to commit identity theft, fraud, theft of services, telephone harassment, and various other offenses. CW1 described Weigman's roll in the conspiracy to me as the individual who was responsible for altering telephone services in furtherance of this scheme.
- e. In the conspiracy, Martinez was responsible for making the harassing calls in furtherance of the scheme, and earned the nickname of "Wicked Wizard".



f. In the conspiracy, Ward was responsible for financing the operations, paying to have others swatted.

g. In the conspiracy, Trowbridge was responsible for using a commercial database to find identifying information about individuals for purposes of targeting them for the subsequent swatting operations.

h. In the conspiracy, **NEFF** was responsible for some of the same things as the others, and operated the partyline gaga website.

i. The “swatting” group used commercial services to disguise and conceal their identities, such as online spoofing services and the purchase of telephone calling cards.

23. Affiant believed CW1 provided reliable information. Affiant conducted records checks and other investigation, and verified a large portion of the information provided by CW1. Affiant believed CW1 had access to the information that CW1 provided. Affiant knows that other members of the party lines have accused CW1 of participating in telephone harassment, Affiant does believe that CW1 has participated in telephone harassment, and therefore is or has been engaged in criminal activity.

24. Affiant investigated SP’s November 2006 information about the web site [www.partylinegugu.com](http://www.partylinegugu.com) (partylinegugu) operated by **NEFF**. Affiant found that partylinegaga was another site name for partylinegugu and that typing either one into an Internet web browser would bring the browser to the same web site. Affiant examined the photos on the web site and located one for “Lupe,” aka Martinez and one for “Michael

Knight,” aka Rosoff. Affiant noted that many of the participants used alias names or nicknames. At the time, Affiant compared the photo for “Michael Knight” to a driver’s license photo of Rosoff. Portland, Oregon FBI agents advised Affiant that they compared an Oregon driver’s license photo of Martinez to the “Lupe” photo on partylinegugu, and it appeared to be the same individual. Affiant determined that partylinegugu was hosted at DrTrendy.com (DrTrendy), a small web hosting company run by Jeffrey Daniels, a.k.a. Jeff Daniels, located at 6 Cornelius Park Dr, Oneonta, AL 35121. SP had previously told Affiant that Jeffrey Daniels was a participant in the chat lines. In July and August 2007, other party line members contacted Affiant and advised Affiant that there were two competing versions of the partyline web site, one run by NEFF, and the other run by Daniels.

25. Affiant also accessed partylinegaga and noted that the photo of a number of the subjects were identified only by aliases or nicknames. Partylinegaga listed Jeff Daniels as the webmaster, and the hosting site as [www.alabamatechsupport.com](http://www.alabamatechsupport.com). Partylinegaga also posted biographical information or “bio pages” on some subjects, and contest pages challenging members to obtain personal information on other subjects.

26. Affiant listened to consensually made recordings of the swatting group in their telephone conference chat on the named party lines from November 2006. In one of the calls, several of the members of the group threatened to have SP “swatted” again. Voices of the callers included Martinez, Ward, and Trowbridge. A member who identified himself as Ward stated that he would pay \$300 per “swat” if someone would “swat” both

SP's parents and siblings. During this discussion, numerous individuals, including one identified by a cooperating party line participant as Martinez were heard laughing about the original "swatting." Discussions among them included the information that Martinez did "swat" SP, but that he did it only after another conspirator offered to pay him to do it.

In what appeared to be an effort to provoke SP, numerous comments were made to the effect that SP's parents had avoided further "swatting" because SP's mother was providing phone sex to Martinez in exchange for him leaving them alone.

27. In December 2006, Weigman, who was then a minor, advised Affiant that he had been participating in the swatting group for over one year and that he was very familiar with the other members of the group. Weigman told me that he had heard a recording of the false 911 call related to the swat of SP and that he recognized the voice in the telephone conference as Martinez. In addition, he had heard multiple conversations discussing the "swatting" of SP in which the members of the group referred to Martinez as the one who had done the "swat." Weigman also stated that Jeffrey Daniels had paid Weigman money for securing Daniels' "network."

28. On January 24, 2007, Affiant met Chad Ward and noted that Ward looked like his photograph on partylinegugu. Ward advised Affiant as follows:

- a. He was a member of the group, but claimed that he had never swatted anyone himself and that his offers of payment had been made in jest.
- b. He wanted to be cooperative as he had already been convicted once for making telephonic bomb threats to a federal courthouse in New York.

- c. He had provided money to the other members of the group, but claimed that the payments were “protection money” to ensure he was not “swatted.”
- d. He had listened in on the 911 phone call when SP was “swatted” and confirmed that Martinez and Trowbridge participated in the call. Ward claimed that Martinez conducted the “swat” but that Trowbridge was the one who had invited Ward to participate in it.
- e. Trowbridge had access to a commercial credit database because his business was a credit business of some type.
- f. Ward had frequent phone conversation with Trowbridge, but added that he had only met with him a few times in person. On one of those occasions Trowbridge had been in Ward’s residence, and Ward had observed Trowbridge access the commercial database from Ward’s downstairs computer and obtain information on other partyline members. Ward provided Affiant with a print out of one of the credit reports that Trowbridge performed.
- g. Once Rosoff and Martinez were arrested Ward had erased the evidence of Trowbridge’s use of his computer.
- h. Trowbridge’s had seven computers at residence.
- i. Trowbridge was aware that Ward recorded the swatting of SP, and became upset and directed Ward to “get rid of” the recording. Ward provided Affiant with voice mail recordings of group members discussing criminal activity such as threats and swatting.

j. Ward had purchased a “spoofcard” using his computers located upstairs in his residence. He used the “spoofcard” to gain unauthorized access to a phone company in order to improve the security level of his and others’ phones. Ward provided the “spoofcard” to Weigman to do the actual work. Later, Weigman provided the card to Rosoff.

k. Ward and Jeffrey Daniels, a.k.a. “JDT” were involved in a chat line business which offered chat services.

29. On January 24, 2007, Affiant went to Trowbridge’s residence. Angela Roberson answered the door, and identified herself as Trowbridge’s girlfriend, and falsely stated that Trowbridge was not home. (Law enforcement found Trowbridge hiding in a closet in the residence). Roberson met with Affiant on this occasion and on subsequent occasions. During the different meetings, Roberson advised Affiant as follows:

- a. She had lived with Trowbridge for three months.
- b. She and Trowbridge were members of the chat room, but claimed that neither she nor Trowbridge ever swatted anyone.
- b. Members would claim they were going to “swat” someone or threaten to do so, in order to maintain their own security and protect against getting “swatted” themselves.
- c. She believed that the computers in Trowbridge’s residence were for use in his business.
- d. Trowbridge ran a debt collection business from his house.

e. Individuals would “pull up records” on other people by computer all the time, but claimed it was in self defense. (Affiant understood this to mean that members of the partyline group obtained personal identifying information of other members).

f. Initially, Roberson stated that she gotten records on others accessing publically available records on the Internet. Later Roberson admitted that she had obtained the records from Accurint, an online commercial database.

g. Roberson used various computers in the residence to communicate with Martinez through Instant Messenger and their respective “MySpace” web pages.

h. Members of the group faked being telephone company employees in order to advance the chat room schemes.

30. At the conclusion of the initial meeting, Affiant seized the computers from Trowbridge’s residence, and searched the computers pursuant to a search warrant.

31. Between January and June 2007, Affiant reviewed evidence seized from the search warrants, records received by consent, conducted interviews of witnesses and victims, and spoke with other law enforcement agencies. Affiant identified over 250 victims who had been harassed by the group, including police, fire departments, hospitals, child protective services, and other first responder / government services agencies who had been called out on under false pretenses, family members, and employers who had been harassed, and over a hundred reports of false emergency calls attributed to the group, some of which had resulted in injuries to the victims, disruptions in services, and hundreds of thousands

of dollars in losses.

32. Following the arrests of Rosoff, Trowbridge, Ward, and Roberson in 2007, victims in California, New York, Texas, and Omaha contacted Affiant and reported that they were being harassed by unindicted coconspirators, including **NEFF**, Weigman, and Nalley. The goal of these harassing phone calls was to coerce and intimidate the victims to not provide information to the FBI. During the harassing phone calls, the caller concealed his/her Caller ID. AT&T and Verizon advised Affiant that the illegal activity was continuing and was now being orchestrated by Weigman and other unindicted co-conspirators.

33. In 2007, several individuals provided information to Affiant about the criminal conduct of the indicted individuals, and some of these individuals stated that they were friends of **NEFF**. The 'friends' of **NEFF** advised Affiant that **NEFF** had not done anything wrong. In August 2007, Affiant advised the 'friends' of **NEFF** that **NEFF**'s activities were under investigation, and requested the 'friends' of **NEFF** to tell **NEFF** to contact Affiant. The 'friends' of **NEFF** later advised Affiant that they had passed on Affiant's message, but **NEFF** did not wish to speak with Affiant. Between August 2007 and February 2009, Little Rock, AR agents advised Affiant that they attempted to locate **NEFF** without success.

34. On August 7, 2007, Roberson told Affiant that she had first met **NEFF** in April 2006, in a party line and that she subsequently met him in person. While in his presence, she and he joined a party line and **NEFF** admitted to swatting "everyone on the party line

in retaliation for his parents being swatted.” During her time with **NEFF**, he admitted to her that he “pulled docs” on other people. Roberson knew this to mean that **NEFF** found identifying information on people and used that to threaten and harass them. Affiant reviewed computer logs of conversations between **NEFF** and Roberson which confirmed Roberson’s information.

35. FBI Agents advised Affiant that on August 17, 2007, JR told them about threats made by **NEFF** against JR’s father, MR. JR had gone to school with **NEFF** and did not know why **NEFF** threatened MR. FBI Agents advised Affiant that on August 20, 2007, MR explained that MR reported **NEFF** and Trowbridge for stealing MR’s identity, and **NEFF** had threatened him in retaliation. Affiant knows such retaliation to be in violation of 18 U.S.C. §1512.

36. In November 2007, AS contacted the FBI to complain that **JASON NEFF** had been “hacking and sabotaging” AS’s web site [www.asteresk.org](http://www.asteresk.org) with losses to AS of \$10,000.

37. In May 2008, WS, a Verizon employee, advised Affiant that Weigman and Nalley were harassing WS and trying to get WS fired in retaliation for WS’s assistance in the swatting investigation and prosecution. WS was a potential witness for the trial in 3:07-CR-196-B. Previously, an AT&T employee advised Affiant that Nalley had attempted to have him/her terminated in retaliation for an internal AT&T investigation into the “swatting” group’s activities prior to the FBI becoming involved. The harassment culminated when Weigman and another party line member, Sean Benton drove across



state lines to WS's house in order to harass and intimidate him. Weigman, Benton, and Nalley were indicted and pled guilty the NDTX in 3:08-CR-171-M for obstruction of justice, in violation of 18 U.S.C. § 1512 and/or 1513.

38. On July 21, 2008, Weigman advised Affiant that since the 2007 indictment (Rosoff et al), he and **NEFF** were worried because they both knew they were targets of the investigation. **NEFF** read aloud court filings on the party line to Weigman, who is visually impaired. Weigman advised Affiant that he and **NEFF** threatened people they suspected were cooperating with the FBI in order to prevent them from continuing to cooperate.

39. In 2008, Benton advised Affiant that **NEFF** committed credit card fraud. Benton provided Affiant with computer logs showing a conversation with **NEFF**'s partner in the fraud indicating that this was the case.

40. Affiant has interviewed or been provided reports by other agents who had interviewed over fifty members of the party line. In these interviews and report, the party line members admitted using a number of party lines in which to commit fraud, swatting, and obstruction, including but not limited to the "Donut," the "Loach," "Studio 55," "The Tuscon," "The Raven," and "Sentura Chat."

41. During the course of this investigation, Affiant has listened to hundreds of recorded conversations. A large number of the recordings were made by party line members during calls and conversations on the party lines. These recordings often contained evidence of the conspiracy, such as harassment of victims, swatting calls,

threats, the relaying of illegally obtained personal information, planning sessions for future offenses, discussions of previous offenses, how best to conduct the activity, how to hide the activity from law enforcement, what to say to avoid prosecution, threats not to cooperate with law enforcement, and attempts to retaliate against witnesses, including: law enforcement personnel; subjects who have cooperated; telecommunications employees who have provided the FBI records; and victims .

42. In April 2010, DS contacted Affiant. Between April 2010 and August 2010, the victim provided the following information:

- a. He/she had been/ was being harassed by three party line members, Ghost Rider, White Jordan, and **Crazy J**. **Crazy J** was known to DS as **JASON NEFF**.
- b. **NEFF** had been living with a female party liner, until she accused **NEFF** of abusing her child. **NEFF** fled to avoid criminal charges.
- c. **NEFF** moved in with party line White Jordan. **NEFF**, White Jordan, and Ghost Rider continued to harass DS .
- d. White Jordan alerted law enforcement as to the fact that **NEFF** was living with him.

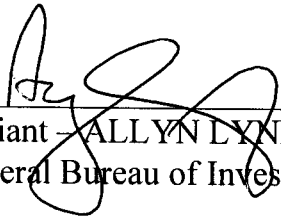
43. In August 2010, Affiant reviewed a criminal history printout and received information from law enforcement in Camden County, Missouri, and determined that **NEFF** was in custody on a state charge of sodomy and child molestation. Additionally, **NEFF** had pending charges out of IOWA for criminal mischief as of 6/29/2010, and being a fugitive from justice as of 8/18/2010.

CONCLUSION


In light of the foregoing, Affiant believes there is probable cause to believe that violations of 18 U.S.C. § 371 (18 U.S.C. §§ 1029(a)(9); 1030(a)(5)(A)(ii); and 1030(a)(2)(A)), and § 1512(k) (18 U.S.C. §§ 1512(b)(3) and 1512(c)(1) and (2)) have been committed by **JASON NEFF** and that there is probable cause to believe that he plans to commit further offenses.

Affiant respectfully request that an arrest warrant be issued authorizing the arrest

**JASON NEFF**, also known as "CrazyJ," "Cl0pz," and "Cl0pz420"  
date of birth xx/xx/1981, Social Security Number xxx-xx-0970,  
(currently incarcerated in Camden County, Missouri, on charges of Sodomy  
and Child Molestation)

  
Affiant - **ALLYN LYND**, Special Agent  
Federal Bureau of Investigation

SWORN TO AND SUBSCRIBED before me this 2nd day of September 2010.

  
**RENEE HARRIS TOLIVER**  
United States Magistrate Judge  
Northern District of Texas